Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of detecting a computer malware comprising the steps of:

joining an Internet Relay Chat server; retrieving a list of channels of the Internet Relay Chat server; monitoring at least one channel in the list of retrieved channels[;], by:

joining a channel,

waiting a time delay,

leaving the channel, and

simulating user activities by transmitting a message to the channel; accepting data received from the monitored channel; and storing and logging the data received from the monitored channel; and

scanning the received data to detect a computer malware.

- 2. 5. (Cancelled)
- 6. (Currently Amended) The method of claim [5]1, wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program.
- 7. (Currently Amended) The method of claim 1, further comprising the step of: analyzing the stored and logged data to detect thea computer malware.
- 8. (Original) The method of claim 7, wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program.

Appl. No. 10/076,441 Reply to Office action of April 7, 2005

9. - 14. (Cancelled)

15. (Currently Amended) A system for detecting a computer malware comprising: a processor operable to execute computer program instructions; a memory operable to store computer program instructions executable by the processor; and

computer program instructions stored in the memory and executable to perform the steps of:

joining an Internet Relay Chat server;
retrieving a list of channels of the Internet Relay Chat server;
monitoring at least one channel in the list of retrieved channels[;], by:
 joining a channel,
 waiting a time delay,
 leaving the channel, and
 simulating user activities by transmitting a message to the channel,
accepting data received from the monitored channel; and
storing and logging the data received from the monitored channel; and

scanning the received data to detect a computer malware.

16. -19.(Cancelled)

- 20. (Currently Amended) The system of claim [19]15, wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program.
- 21. (Currently Amended) The system of claim 15, further comprising the step of: analyzing the stored and logged data to detect thea computer malware.
- 22. (Original) The system of claim 21, wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program.

23. - 28. (Cancelled)

29. (Currently Amended) A computer program product <u>embodied on a computer</u> readable medium for detecting a computer malware comprising:

a computer readable medium;

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of

joining an Internet Relay Chat server;

retrieving a list of channels of the Internet Relay Chat server;

monitoring at least one channel in the list of retrieved channels[;], by:

joining a channel,

waiting a time delay,

leaving the channel, and

simulating user activities by transmitting a message to the channel;

accepting data received from the monitored channel; and storing and logging the data received from the monitored channel; and scanning the received data to detect a computer malware.

30. - 33. (Cancelled)

- 34. (Currently Amended) The computer program product of claim [33]29, wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program.
- 35. (Currently Amended) The computer program product of claim 29, further comprising the step of:

analyzing the stored and logged data to detect thea computer malware.

- 36. (Original) The computer program product of claim 35, wherein the computer malware comprises at least one of a computer virus, a computer worm, or a computer Trojan horse program.
- 37.-57. (Cancelled)
- 58. (New) The method of claim 1, wherein transmitting the message to the channel is utilized for triggering the computer malware in the channel to be sent.
- 59. (New) The method of claim 1, wherein the storing and logging includes storing and logging a receipt time of the data and a sender of the data.
- 60. (New) The method of claim 1, wherein an Internet Relay Chat client is utilized in the joining, the retrieving, and the monitoring.
- 61. (New) The method of claim 60, wherein the Internet Relay Chat client automatically accepts and stores the data received from the monitored channel.
- 62. (New) The method of claim 61, wherein the Internet Relay Chat client scans the received data to detect the computer malware.
- 63. (New) The method of claim 62, wherein the Internet Relay Chat client collects statistics.
- 64. (New) The method of claim 63, wherein the Internet Relay Chat client notifies an administrator of the computer malware.
- 65. (New) The method of claim 1, wherein the received data includes direct client-toclient DCC send requests.
- 66. (New) The method of claim 7, wherein the analyzing is automatically performed.

Appl. No. 10/076,441 Reply to Office action of April 7, 2005

67. (New) The method of claim 7, wherein the analyzing is performed manually.